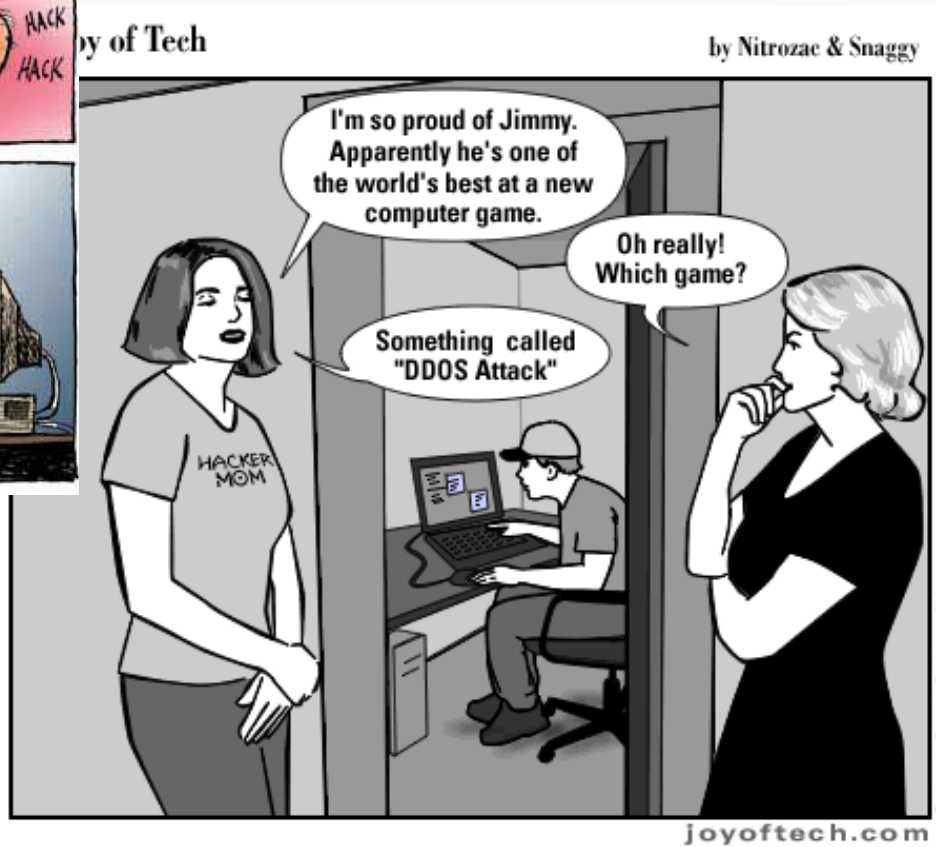
# Anti-DDOS (at) RedIRIS

***Francisco Monserrat***

***Connecting Spanish R&D&i since 1988***

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
MINISTERIO DE ECONOMÍA Y EMPRESA
RedIRIS
red.es
Infraestructuras Científicas y Técnicas Singulares

# DDOS a new security problem ?

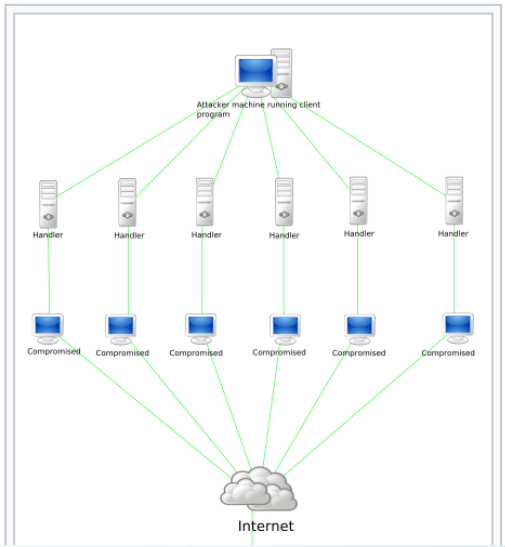



# Denial-of-service attack

From Wikipedia, the free encyclopedia

> *"DoS" redirects here. For the family of computer operating systems, see DOS. For the United States federal executive department, see United States Department of State. For other uses, see DOS (disambiguation).*

In computing, a **denial-of-service attack** (**DoS attack**) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.[1]




In a **distributed denial-of-service attack** (**DDoS attack**), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

A DoS or DDoS attack is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, disrupting trade.

Has your organization received a Denied of Service (DOS) attack in the last year ?

# Why we care about DDOS ?

## Collateral damage

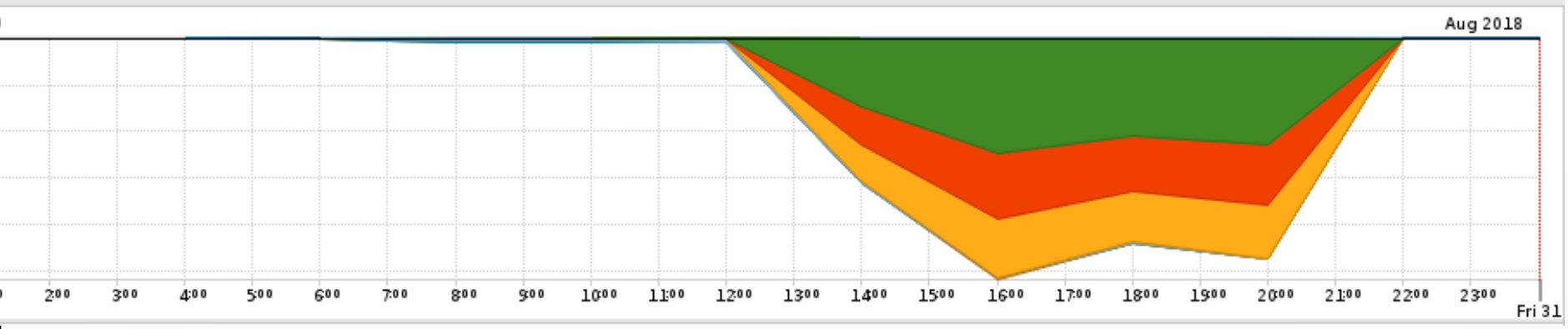
From Wikipedia, the free encyclopedia

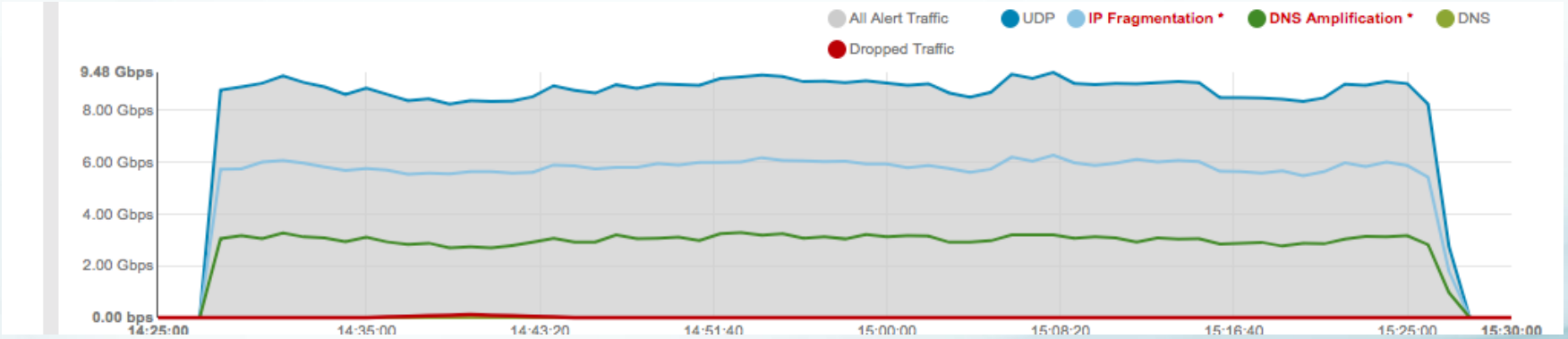
*For other uses, see Collateral damage (disambiguation).*

The examples and perspective in this article **deal primarily with the United States and do not represent a worldwide view of the subject**. You may improve this article, discuss the issue on the talk page, or create a new article, as appropriate.
*(March 2018) (Learn how and when to remove this template message)*

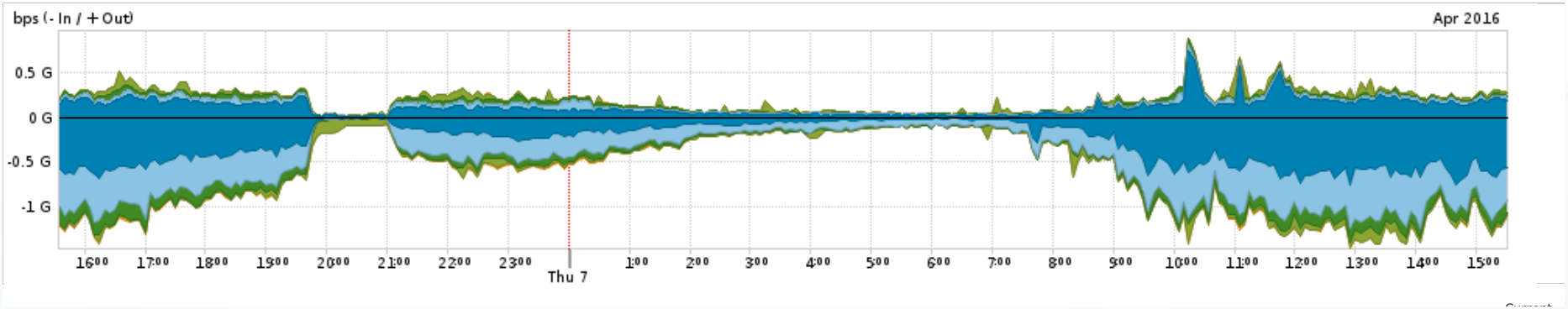
**Collateral damage** is the deaths, injuries, or other damage inflicted on an unintended target. In American military terminology, it is used for the incidental killing or wounding of non-combatants or damage to non-combatant property during an attack on a legitimate military target.[1][2] In US military terminology, the unintentional destruction of allied or neutral targets is called friendly fire.

# Volumetric (data volume) attacks

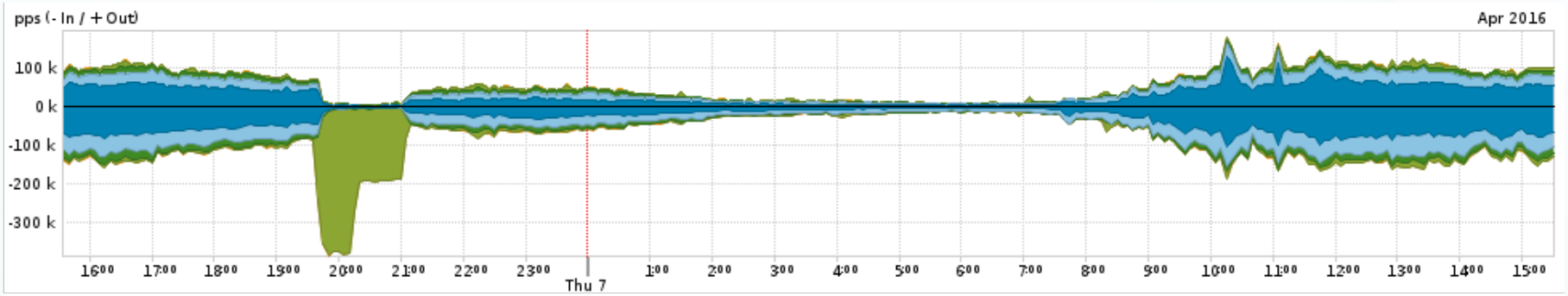


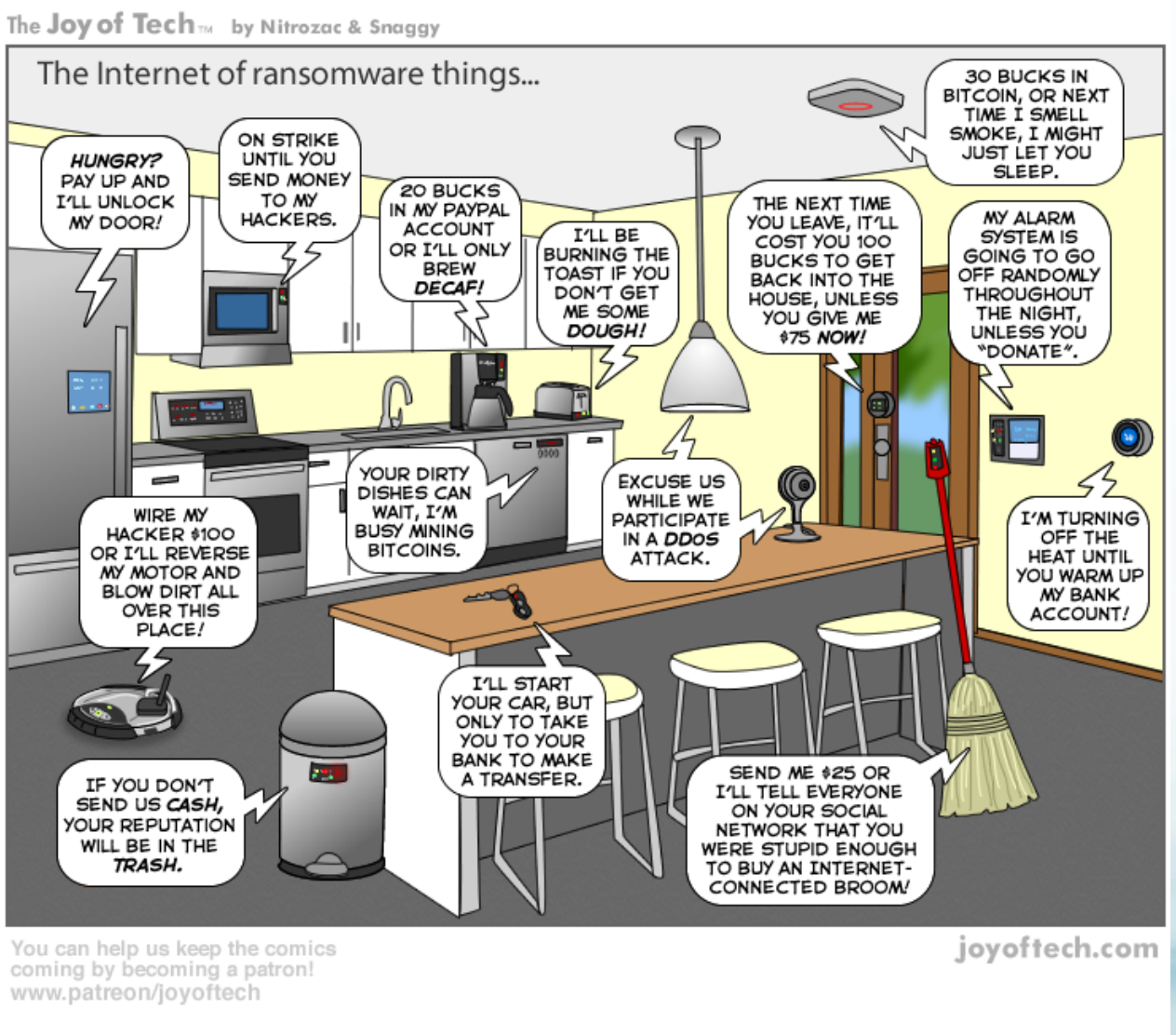
# Non volumetric attacks



# Non volumetric attacks



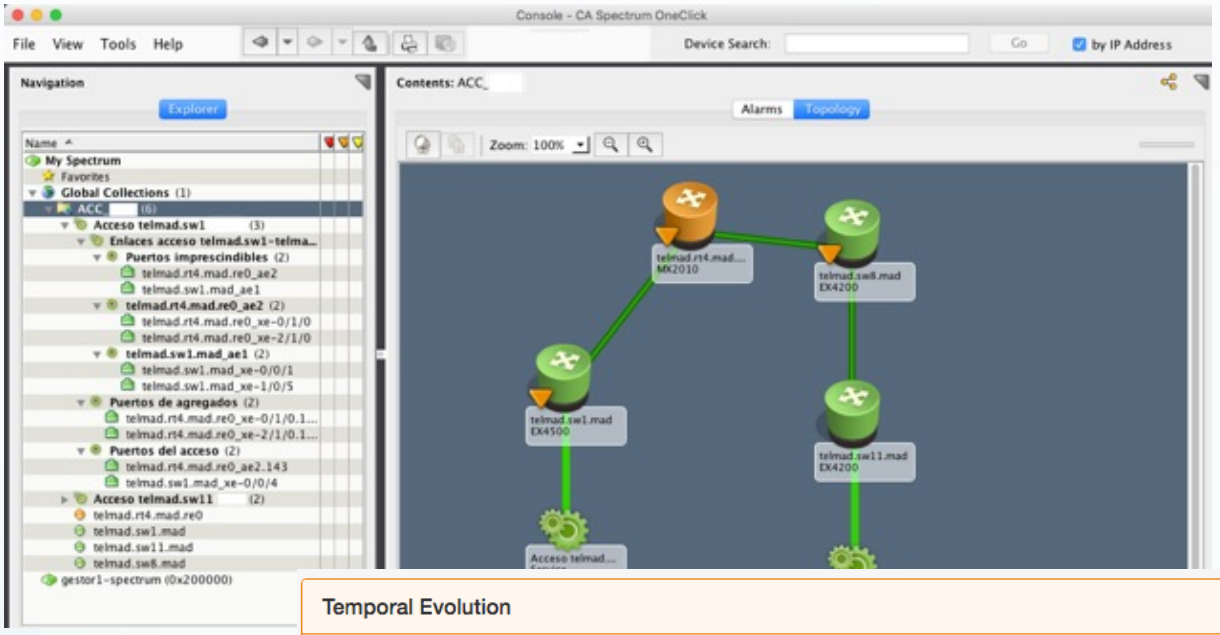
# Non volumetric attacks

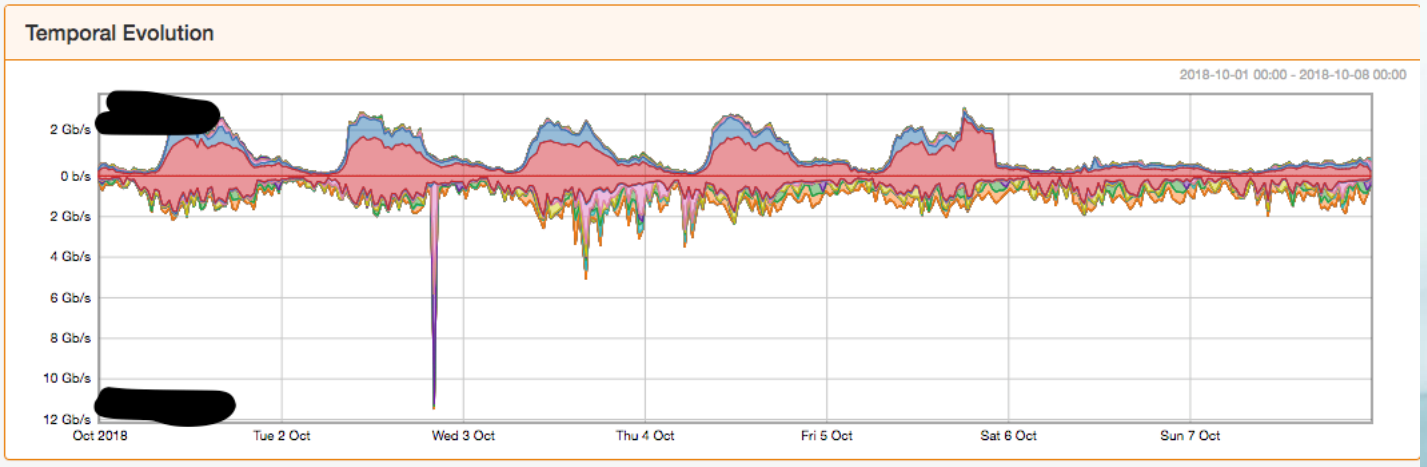


# How do you detect a DOS ?

- Social media ,
- SIEM correlation
- User calling
- Outside call
- Post Morten analysis

# Network information



# Mitigation & cure

Merriam-Webster SINCE 1828

cure

DICTIONARY THESAURUS

**cured**; **curing**

## Definition of *cure* (Entry 2 of 3)

*transitive verb*

1 **a** : to restore to health, soundness, or normality
// *cured* him of a rare blood disease

**b** : to bring about recovery from
// *cure* a disease

2 **a** : to deal with in a way that eliminates or rectifies
// ... his small size, which time would *cure* for him ...
— William Faulkner

**b** : to free from something objectionable or harmful
// trying to *cure* him of a bad habit

SINCE 1828

mitigate

DICTIONARY THESAURUS

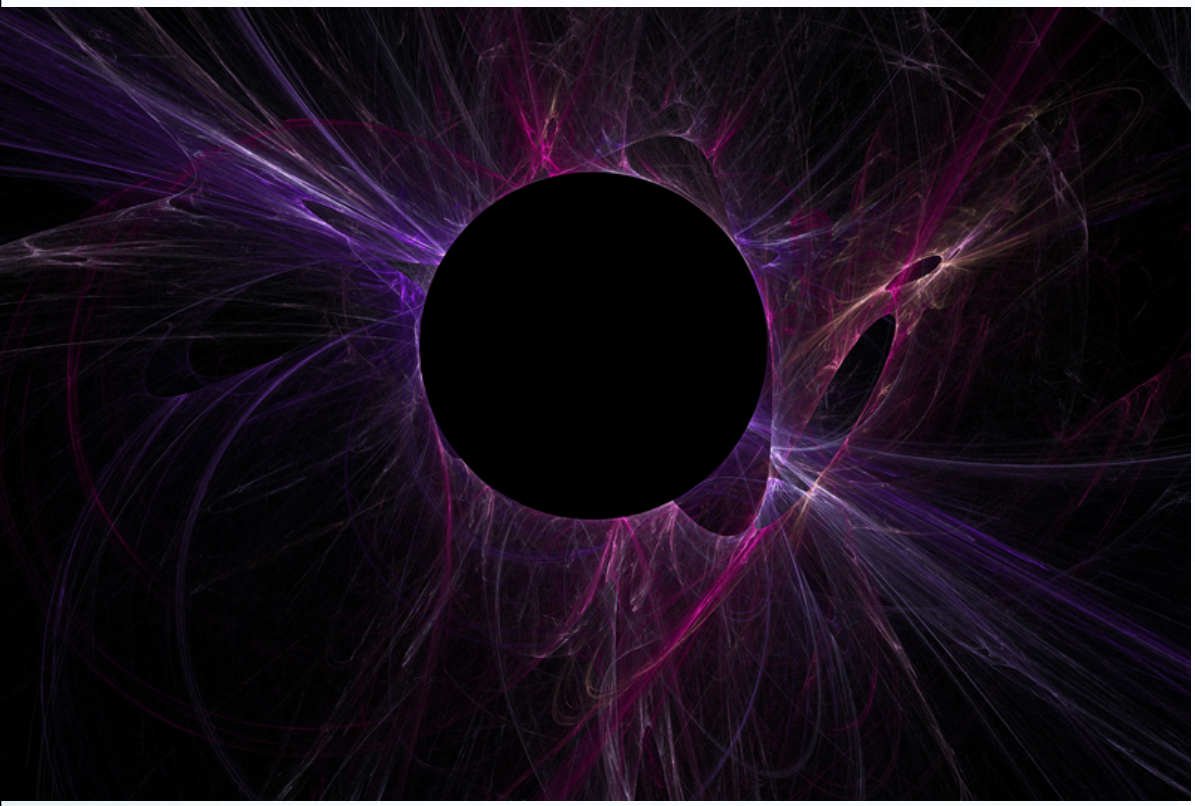
*transitive verb*

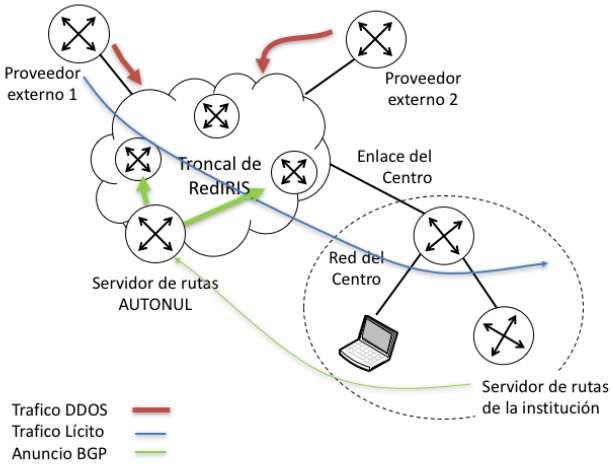
1 : to cause to become less harsh or hostile : MOLLIFY
// aggressiveness may be *mitigated* or ... channeled
— Ashley Montagu

2 **a** : to make less severe or painful : ALLEVIATE
// *mitigate* a patient's suffering

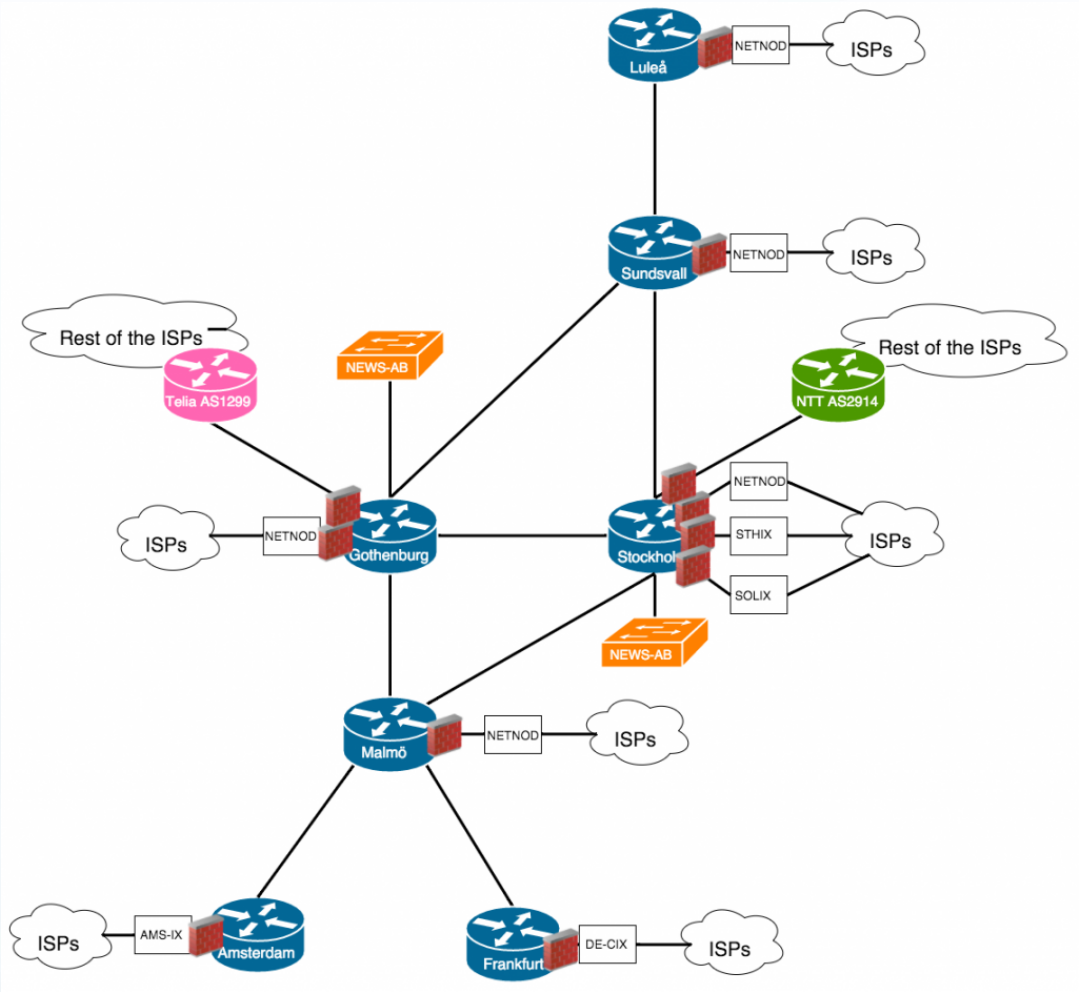
**b** : EXTENUATE
// attempted to *mitigate* the offense

# Blackhole

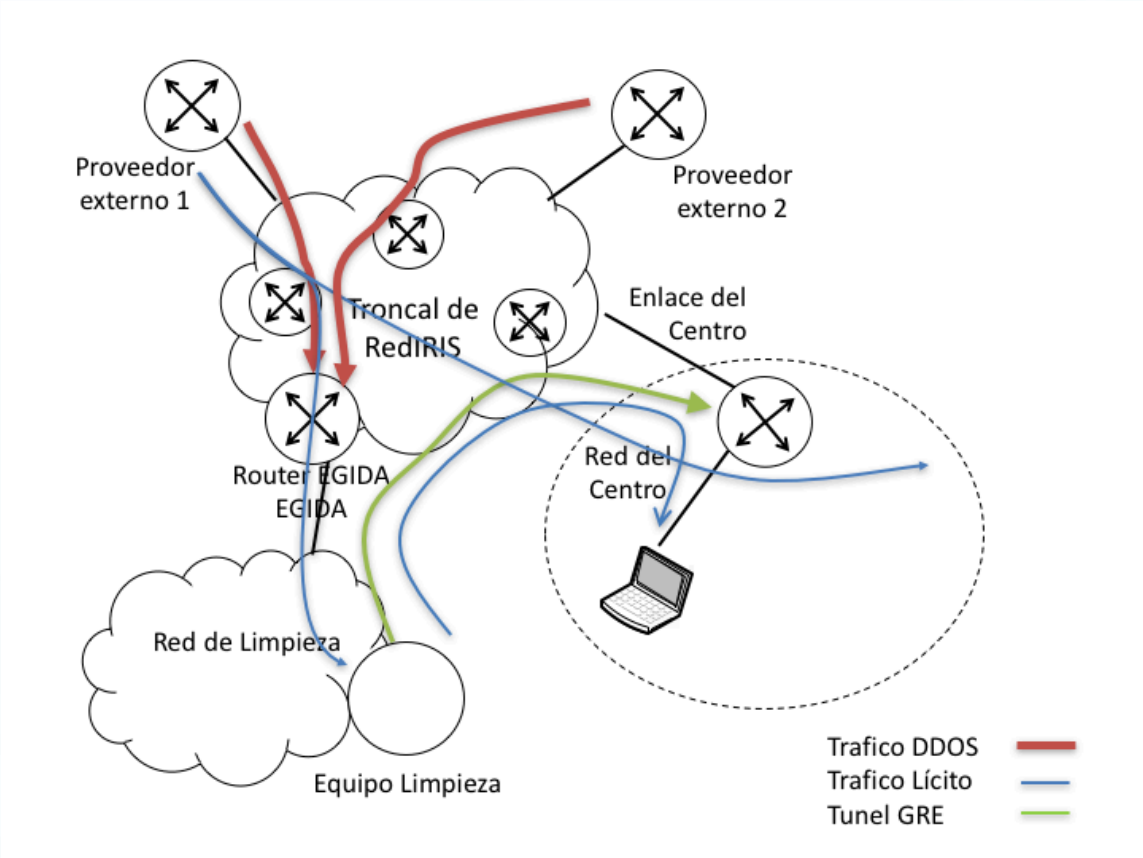



Proveedor externo 1
Proveedor externo 2
Troncal de RedIRIS
Enlace del Centro
Red del Centro
Servidor de rutas AUTONUL
Servidor de rutas de la institución
Trafico DDOS
Trafico Lícito
Anuncio BGP

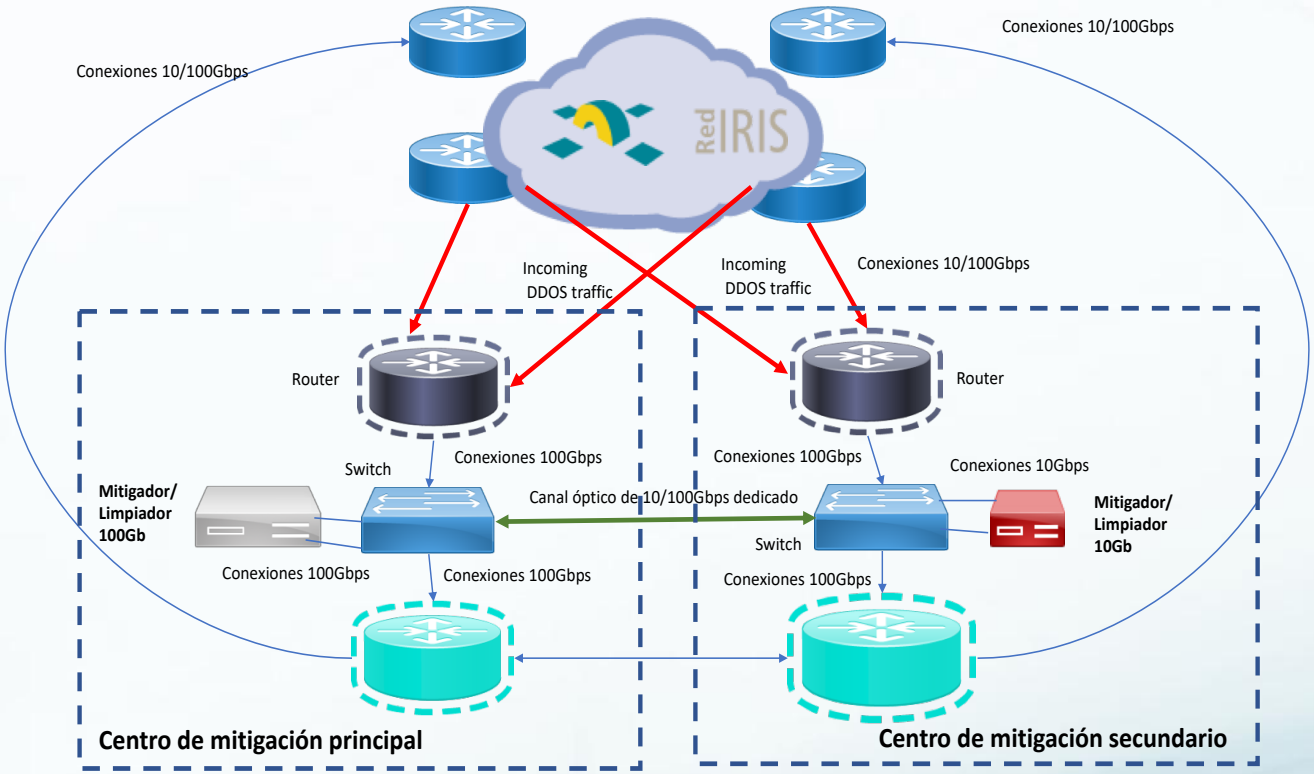
# FlowSpec filtering



# Scrubbing center



# Scrubbing Center



# Timeline


- Tener launched
- New system deploymnet
- Advanced guarantee
- Visualization tender
- Flowspec testing
- End of advanced guaranteee
- Visualization deployment
- Flowspec service

Red IRIS

# THANK YOU VERY MUCH!